C4ISR ARCHITECTURES

The Objective Force Key Enabler

Steve Klynsma and
MAJ Thomas Scott, UK

Introduction

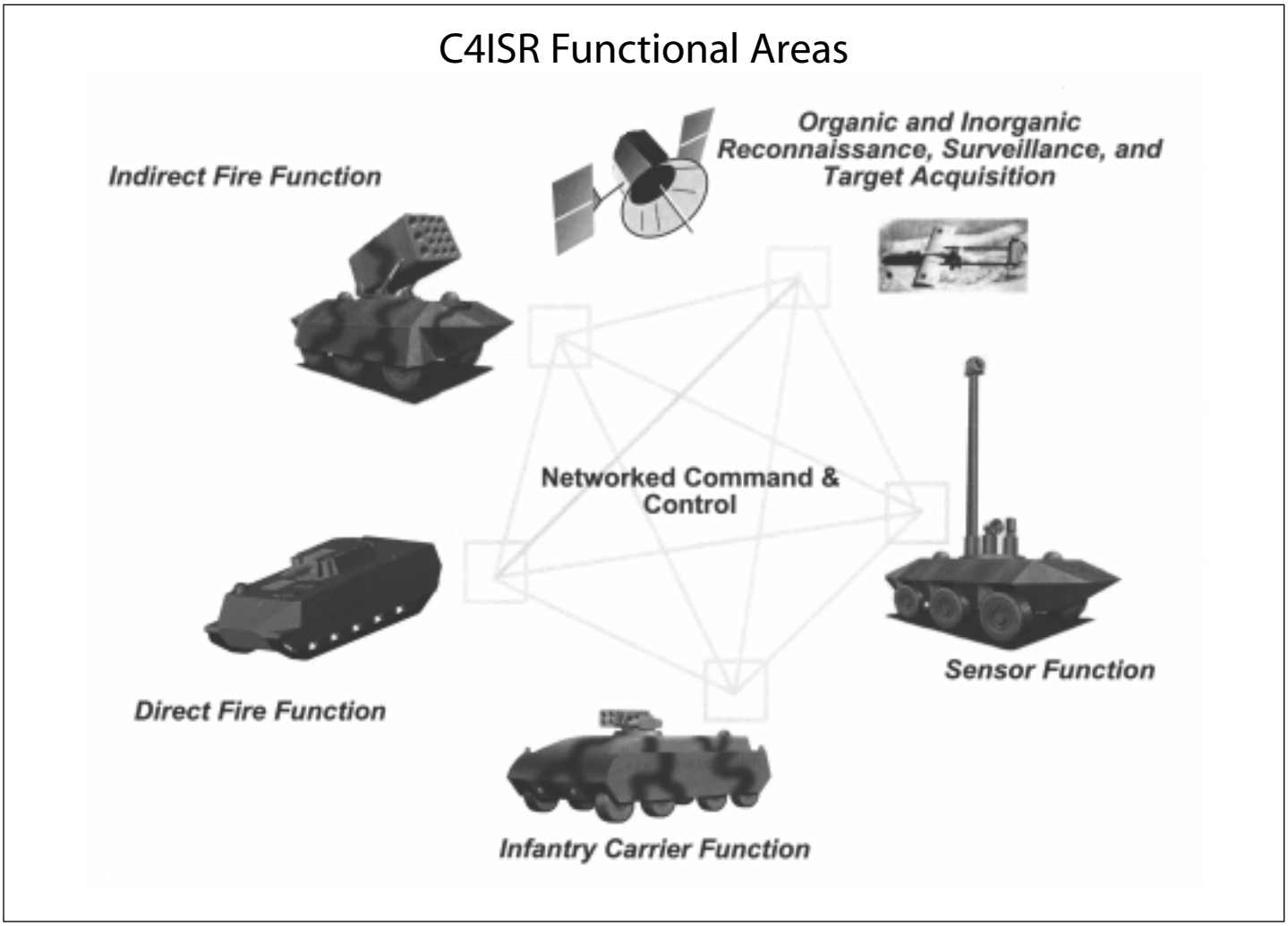
Advances in weapon lethality, as envisioned for the Objective Force, have traditionally necessitated the development of heavier or more technologically advanced armor to protect the warfighter. However, to meet its strategic goals, the Objective Force must provide lethal combat overmatch with less weight and greater agility. This requires the Army to move from a platform-centric to a network-centric architecture, providing greater situational awareness. This situational understanding, along with greater mobility, more lethal precision weapons, and integrated joint capabilities, will obviate the Army's traditional reliance on heavy armor for force protection. Multifunctional weapon systems within Future Combat Systems (FCS) are key, but the real revolution in warfighting brought about by the Objective Force is the integrated, multitiered command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) network. Battles will be won or lost based on the network's ability to provide the situational picture allowing the commander to see and understand first.

A Different Architecture

C4ISR architecture for the Objective Force will be substantially different from the architecture of today's tactical communications infrastructure. Current architectures rely on a stable, semifixed supporting infrastructure established on elevated terrain. Relocating elements (signal nodes) of this infrastructure is not trivial and often results in lengthy periods of degraded communications. During these periods, the commander risks losing touch with the flow of the battle. The Army science and technology community is developing new technologies supporting command and control (C2) on-the-move. These technologies will free commanders from today's rigid infrastructure and allow them to focus on the battle. Commanders will be able to roam the battlefield at will, continually maintain situational awareness data feeds, and effortlessly direct subordinate commanders.

The architecture of the Objective Force C4ISR network will include mechanisms for graceful degradation, dynamic reallocation of spectrum and bandwidth, information assurance, authentication, and autoconfiguration. It will be high-bandwidth, long-range, robust (e.g. anti-jam), secure (anti-hacker), and covert. The FCS will also depend heavily on the C4ISR network tying together its major functional areas of direct fire, indirect fire, infantry assault, intelligence, and reconnaissance. The architecture will enable collaborative fires (both direct and indirect) and reduce sensor-to-shooter timelines. The Objective Force Unit of Action will have organic C4ISR assets that permit unrestricted operations anywhere in the world. The network must be of sufficient reliability and robustness to permit simultaneous multiuser and multiprecedent connectivity. Obviously, as with the earlier commander's scenario, such connectivity requires terrain-independence. Therefore, the Objective Force C4ISR architecture will include satellite and airborne communication nodes, as well as the more traditional terrestrial links, providing network connectivity and range extension.

The Objective Force will operate in a geostrategic environment encompassing a trend toward a nonlinear, multidimensional battlespace. The emphasis will not only be on joint interdependence and combined interoperability, but also on an inherent capability to interact with nongovernmental organizations, private volunteer organizations, and indigenous infrastructures. Internetted "systems-of-systems" that operate seamlessly across the tactical, operational, and strategic levels will be key, including a robust and large reach-back capability that enables split-based operations. CONUS-based "sanctuaries" will facilitate interagency collaboration while providing a portal to the tactical arena. Command, control, communications, and computers (C4) information technologies thus arguably become the most significant common denominators across all the technologies and concepts being considered for the Objective Force.



Infrastructure

To understand and manage the complexity of the networks required for the Objective Force, the Army is beginning to document the architectural infrastructure supporting it. Architectures provide a mechanism for understanding and managing complexity. The DoD C4ISR Architecture Framework Document Version 2.0 defines architecture as "*the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time*." C4ISR architecture provides for the examination of processes and system implementations in the context of mission operations and information requirements. Architectures are generally composed of three specific views, which to be consistent and integrated, must have explicit linkages between them. Such linkages are also needed to provide a cohesive audit trail from integrated mission operational requirements and measures of effectiveness to the supporting systems and their characteristics, and to the specific technical criteria governing the acquisition and development of the supporting systems. The three typical architecture views are as follows:

• The *operational view* describes the tasks and activities, operational elements, and information flows required to accomplish or support a mission or functional area. Operational views are generally independent of organization, force structures, and technology.

• *System views* depict the functional and physical automated systems, nodes, platforms, communication paths, and other critical elements that support the information-exchange requirements and warfighter tasks described in the operational architecture views.

• The *technical view* is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements. Technical views facilitate integration and promote interoperability across systems and compatibility among related architectures. Essentially, they prescribe the technical implementation standards and conventions—such as building codes—on which the architecture depends.

Grids

C4ISR architecture will form the backbone of the FCS and the Objective Force and will enable the effective application of all other capabilities, including operational movement

and maneuver, tactical maneuver, vertical envelopment, mobile strike, and close combat. The Objective Force C4ISR architecture will need to encompass logical sensor, information, and engagement grids, which are internetted via a physical communications grid to provide a virtual internetted C4ISR infosphere. This seamless integration at multiple levels will involve information exchange interfaces to support mission planning across echelons, sensor information for battlespace awareness, and beyond-line-of-sight targeting.

The sensor grid will logically connect organic manned, unmanned, remote, platform, and soldier sensors along with nonorganic Army, joint, and coalition capabilities. A ubiquitous and robust sensor grid will contribute significantly to a more comprehensive and more accurate joint common operating picture, locate key enemy capabilities for destruction, enable reliable battle damage assessment, and enhance the ability of the commander to employ forces more effectively. Improved situational understanding provided by the sensor grid will also strengthen survivability and force protection, allowing the force to preserve combat power.

The information grid will logically provide commanders at all echelons with sophisticated battlespace management tools and capabilities to transform battlespace awareness and understanding into executable actions. Advanced C4ISR capabilities, including automated decision aids and collaboration tools, will enable commanders to make qualitatively better decisions faster than the enemy, thus thwarting the enemy's ability to respond.

The engagement grid will leverage enhanced battlespace awareness, engagement quality target information, distributed battle damage assessment sensors, and shared knowledge of the commander's intent to plan and execute synchronized lethal and nonlethal effects on the adversary. Like the sensor and information grids, the engagement grid is a logical construct enabling coordinated and collaborative fires, dependent on the communications grid.

The communications grid will provide a ubiquitous "always-on" virtual back-plane to support communications among all battlefield entities. Extended range and redundant communication networks will expand the commander's reach and ensure continuous connectivity via multiple pathways. The global information infrastructure in which the Objective Force will function must provide ubiquitous data transport and information to the warfighter, independent of location, degree of mobility, or platform dynamics. The information infrastructure will use a heterogeneous mixture of available media including civilian fiber optic cable plants; landlines; and terrestrial, airborne, and satellite-based wireless services. This infrastructure will likely be a mix of both civilian and military systems. The communications grid will be supported by the emerging Warfighter Information Network-Tactical and the Joint Tactical Radio System.

Conclusion

The C4ISR architecture must provide for the integration of all these systems into a seamless, dynamic, and extensible information transport system that is scalable and has security appropriate to the military mission and the information warfare threat. A C4ISR architecture provides the only truly integrating mechanism for the Objective Force information requirements discussed. It incorporates information technology consistently, controlling the configuration of technical components and ensuring compliance with technical "building codes" through the use of interdependent views. The development of this architecture will be evolutionary as concepts and technology increase in fidelity over time. The multilevel C4ISR architecture will provide an essential mechanism for understanding and managing the extremely complex requirements, standards, and implementation details of the Objective Force.

STEVE KLYNSMA is a Lead Network Engineer working for The MITRE Corp. in support of the Army Office of the Director of Information Systems for Command, Control, Communications, and Computers. He graduated from the U.S. Military Academy in 1983 and has an M.S. in communications and computers from The George Washington University.

MAJ THOMAS SCOTT is the United Kingdom (U.K.) Exchange Officer in the Office of the Director of Information Systems for Command, Control, Communications, and Computers. He was educated at Glasgow University, Cranfield University, and Kings College London. He has a B.S. in mechanical engineering with a specialization in engineering management, an M.S. in the design of information systems, and an M.A. in defense studies. He is also a graduate of the U.K. Joint Services Command and Staff College.
